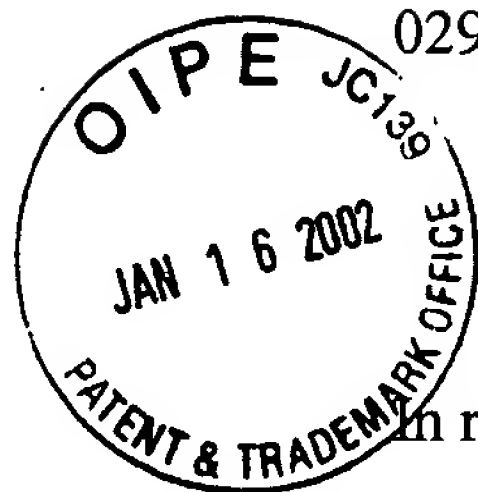


#3

02985.000374

PATENT APPLICATION



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

NAOYUKI OE ET AL.

Application No.: 09/988,106

Filed: November 19, 2001

For: INFORMATION PROCESSING
METHOD, APPARATUS, AND
SYSTEM FOR CONTROLLING
COMPUTER RESOURCES,
CONTROL METHOD
THEREFOR, STORAGE MEDIUM,
AND PROGRAM

Examiner: Not Yet Assigned

Group Art Unit: 2152

January 15, 2002

Commissioner for Patents
Washington, D.C. 20231

RECEIVED
JAN 17 2002
Technology Center 2100

CLAIM TO PRIORITY

Sir:

Applicants hereby claim priority under the International Convention and all rights to which he is entitled under 35 U.S.C. § 119 based upon the following Japanese Priority Applications:

2000-352113 filed on November 20, 2000

2001-161403 filed on April 23, 2001

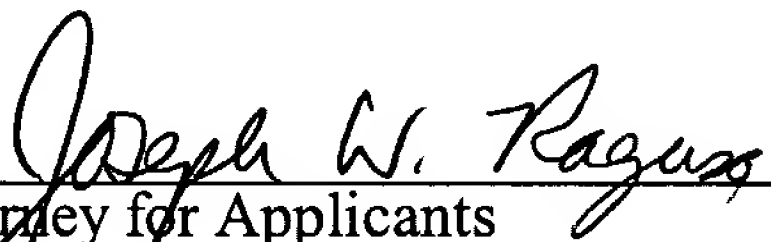
2001-190445 filed on May 22, 2001

2001-322437 filed on October 19, 2001

Certified copies of the priority documents are enclosed.

Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our address given below.

Respectfully submitted,


Attorney for Applicants
Registration No. 38,586

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

NY_MAIN 231323 v 1

(Translation of the front page
of the priority document of
Japanese Patent Application
No. 2000-352113)

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of
the following application as filed with this Office.

Date of Application : November 20, 2000
Application Number : Patent Application
2000-352113
Applicant(s) : Humming Heads Inc.

RECEIVED
JAN 17 2002
Technology Center 2100

November 9, 2001

Commissioner,
Japan Patent Office

Kouzo Oikawa

Certification Number 2001-3098287

日 本 国 特 許 庁
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年11月20日

出 願 番 号

Application Number:

特願2000-352113

出 願 人

Applicant(s):

ハミングヘッズ株式会社

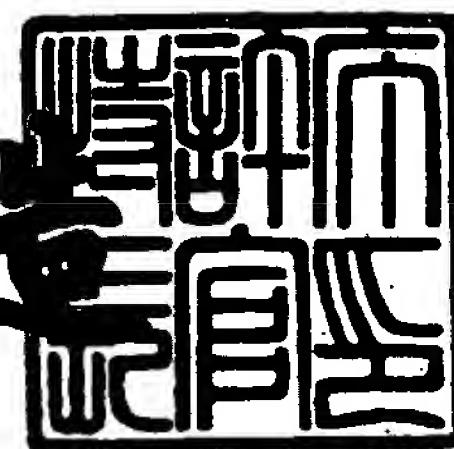
RECEIVED
JAN 17 2002
Technology Center 2100

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年11月 9日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3098287

【書類名】 特許願

【整理番号】 HH00001

【提出日】 平成12年11月20日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00

【発明者】

 【住所又は居所】 東京都中央区月島一丁目2番13号 ハミングヘッズ株式会社内

 【氏名】 大江 尚之

【発明者】

 【住所又は居所】 東京都中央区月島一丁目2番13号 ハミングヘッズ株式会社内

 【氏名】 志摩 貴浩

【特許出願人】

 【識別番号】 500083226

 【氏名又は名称】 ハミングヘッズ株式会社

【代理人】

 【識別番号】 100088720

 【弁理士】

 【氏名又は名称】 小川 眞一

 【電話番号】 03-3256-8439

【手数料の表示】

 【予納台帳番号】 052504

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンピュータリソースの制御方法および装置並びに記録媒体

【特許請求の範囲】

【請求項 1】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御する方法であって、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 1 のステップと、

前記第 1 のステップで捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第 2 のステップと、

アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第 3 のステップと、

アクセス権限がなければ当該操作要求を拒否する第 4 のステップとを備えることを特徴とするコンピュータリソースの制御方法。

【請求項 2】 前記第 1 のステップに代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 5 のステップを備えることを特徴とする請求項 1 に記載のコンピュータリソースの制御方法。

【請求項 3】 前記第 2 のステップが、

特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定するステップまたは、

コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定するステップまたは、

アクセス権限が獲得できたか否かをもち、アクセス権限があるか否かを判定するステップ

を備えることを特徴とする請求項 1 または 2 に記載のコンピュータリソースの制御方法。

【請求項 4】 前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも 1 つを指定する情報を含むことを特徴とする請求項 3 に記載のコンピュータリソースの制御方法。

【請求項 5】 前記第 4 のステップは、

要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返すステップから成ることを特徴とする請求項 1 ～ 4 のいずれか一項に記載のコンピュータリソースの制御方法。

【請求項 6】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御するリソース制御手段を備えたコンピュータ装置であって、

前記リソース制御手段が、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 1 の手段と、

前記第 1 の手段で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第 2 の手段と、

アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第 3 の手段と、

アクセス権限がなければ当該操作要求を拒否する第 4 の手段とを備えることを特徴とするコンピュータ装置。

【請求項 7】 前記第 1 の手段に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 5 の手段を備えることを特徴とする請求項 6 に

記載のコンピュータ装置。

【請求項 8】 前記第 2 の手段が、

特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定する手段または、

コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定する手段または、

アクセス権限が獲得できたか否かをもち、アクセス権限があるか否かを判定する手段

を備えることを特徴とする請求項 6 または 7 に記載のコンピュータ装置。

【請求項 9】 前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも 1 つを指定する情報を含むことを特徴とする請求項 8 に記載のコンピュータ装置。

【請求項 10】 前記第 4 の手段は、

要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す手段から成ることを特徴とする請求項 6 ～ 9 のいずれか一項に記載のコンピュータ装置。

【請求項 11】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスを制御するリソース制御プログラムを記録した媒体であって、

前記リソース制御プログラムが、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 1 の処理

と、

前記第 1 の処理で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第 2 の処理と、

アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第 3 の処理と、

アクセス権限がなければ当該操作要求を拒否する第 4 の処理とを備えることを特徴とするコンピュータが読取り可能なプログラムを記録した記録媒体。

【請求項 1 2】 前記第 1 の処理に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 5 の処理を備えることを特徴とする請求項 1 に記載の記録媒体。

【請求項 1 3】 前記第 2 の処理が、

特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定する処理または、

コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定する処理または、

アクセス権限が獲得できたか否かをもち、アクセス権限があるか否かを判定する処理

を備えることを特徴とする請求項 1 1 または 1 2 に記載の記録媒体。

【請求項 1 4】 前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも 1 つを指定する情報を含むことを特徴とする請求項 1 3 に記載の記録媒体。

【請求項 1 5】 前記第 4 の処理は、

要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知

を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理から成ることを特徴とする請求項 1 1 ～ 1 4 のいずれか一項に記載の記録媒体。

【請求項 1 6】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスを制御するリソース制御プログラムであって、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 1 の処理と、

前記第 1 の処理で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第 2 の処理と、

アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第 3 の処理と、

アクセス権限がなければ当該操作要求を拒否する第 4 の処理とを備えることを特徴とするコンピュータが実行可能なリソース制御プログラム。

【請求項 1 7】 前記第 1 の処理に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第 5 の処理を備えることを特徴とする請求項 1 6 に記載のリソース制御プログラム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、ファイル、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスを管理するコンピュータリソースの制御方法および装置並びに記録媒体に関するものである。

【 0 0 0 2 】

【従来の技術】

従来において、パーソナルコンピュータ等のコンピュータにおけるファイルや記憶装置等のリソースをアプリケーションプログラムを介してユーザがアクセスする場合に、アクセス権限のないユーザに情報が解読または盗聴されるのを防ぐために、オペレーティングシステム（以下、OS）内にアクセス権限のチェック機能を設ける方法、あるいは専用のアクセス管理ツールを付加してアクセス権限のチェックを行なう方法が知られている。

【 0 0 0 3 】

例えばWindows（米国マイクロソフト社の登録商標）に代表される汎用のOSにおいては、ファイルの読取り、書き込み、実行をアクセス権限のないユーザに対しては許可しない機能が備わっている。また、ファイルの削除、アクセス権限の変更、所有権の変更についての権限を設定可能にした汎用OSもある。

また、アクセス管理ツールとして、例えば特開平7-84852公報に開示されているように、ファイルの参照と共に複写の可否を登録し、その可否によって参照、複写を制限するものが知られている。詳しくは、表示領域に読出し制限の属性を付加し、表示画面のハードコピーを防止するものが知られている。

【 0 0 0 4 】

【発明が解決しようとする課題】

アクセス権限のないユーザに対して情報の持ち出しを全面的に禁止するためには、図9に示すように、メールへの添付、印刷、ファイル移動／ファイルコピー、クリップボードへのコピー、フロッピーディスクへの別名保存、オブジェクトの貼り付け、キャプチャーなどの機能を制限する必要がある。さらに、ネットワークを通じた情報の持ち出しを制限する必要がある。

しかしながら、上記従来技術にあっては、ファイル及び画面のハードコピー以外の操作（例えばクリップボードへのコピー）に対して制限することができないという問題がある。もしも、クリップボードへのコピーなどの操作を制限しようとする場合には、OSまたはアプリケーション自体に変更を加えることが必要になり、汎用的な応用ができないという問題がある。

【 0 0 0 5 】

本発明の目的は、OSやプロセス（OSの元に稼動しているプログラムであり

、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限し、しかも既存環境における禁止または制限事項を拡張することができるコンピュータリソースの制御方法および装置並びに記録媒体を提供することにある。

【0006】

【課題を解決するための手段】

上記目的を達成するために、本発明のコンピュータリソースの制御方法は、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第1のステップと、前記第1のステップで捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第2のステップと、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第3のステップと、アクセス権限がなければ当該操作要求を拒否する第4のステップとを備えることを特徴とする。

また、前記第1のステップに代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第5のステップを備えることを特徴とする。

また、前記第2のステップが、特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定するステップ、またはコンピュータリソース内部に記述された既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定するステップ、またはアクセス権限が獲得できたか否かをもち、アクセス権限があるか否かを判定するステップを備えることを特徴とする。

また、前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限

、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも1つを指定する情報を含むことを特徴とする。

また、前記第4のステップは、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返すステップから成ることを特徴とする。

【 0 0 0 7 】

さらに、コンピュータリソースに対するアクセスを制御するリソース制御手段を備えた本発明に係るコンピュータ装置は、

前記リソース制御手段が、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第1の手段と、前記第1の手段で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第2の手段と、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第3の手段と、アクセス権限がなければ当該操作要求を拒否する第4の手段とを備えることを特徴とする。

また、前記第1の手段に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第5の手段を備えることを特徴とする。

また、前記第2の手段が、特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権があるか否かを判定する手段、またはコンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権があるか否かを判定する手段、またはアクセス権限が獲得できたか否かをもち、アクセス権があるか否かを判定する

手段を備えることを特徴とする。

また、前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも1つを指定する情報を含むことを特徴とする。

また、前記第4の手段は、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す手段から成ることを特徴とする。

【0008】

さらに本発明に係るリソース制御プログラムを記録した媒体は、前記リソース制御プログラムが、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第1の処理と、前記第1の処理で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第2の処理と、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第3の処理と、アクセス権限がなければ当該操作要求を拒否する第4の処理とを備えることを特徴とする。

また、前記第1の処理に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第5の処理を備えること特徴とする。

また、前記第2の処理が、特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権があるか否かを判定する処理、またはコンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権があるか否かを判定する処理、またはア

クセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定する処理

を備えることを特徴とする。

また、前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも1つを指定する情報を含むことを特徴とする。

また、前記第4の処理は、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理から成ることを特徴とする。

【0009】

さらにコンピュータリソースに対するアクセスを制御する本発明に係るリソース制御プログラムは、前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第1の処理と、前記第1の処理で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第2の処理と、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第3の処理と、アクセス権限がなければ当該操作要求を拒否する第4の処理とを備えることを特徴とする。

また、前記第1の処理に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第5の処理を備えることを特徴とする。

【0010】

【発明の実施の形態】

以下、本発明の実施の形態を図面により詳細に説明する。

図1(a)，(b)は本発明を実施する環境の一実施の形態を示すハードウェア構成図である。

図 1 (a) に示す構成は、スタンドアロン構成におけるコンピュータ 1 0 1 のハード構成を示すものであり、ハードディスク (HDD) 1 0 1 1 を備えたパーソナルコンピュータ (PC) 1 0 1 2、ディスプレイ 1 0 1 3、プリンタ 1 0 1 4、外部にリソースデータを出力することが可能な外部装置 1 0 1 5 で構成されている。

パーソナルコンピュータ 1 0 1 2 には、汎用の OS とアプリケーションが組み込まれており、さらに本発明に係るリソース管理プログラムが組み込まれている。

図 1 (b) は、ネットワーク 1 0 2 を利用する場合の構成を示すものであり、図 1 (a) に示したのと同様な構成のコンピュータ 1 0 1 a ~ 1 0 1 c がネットワーク 1 0 2 で接続されている。

【 0 0 1 1 】

このような構成において、一般的に、アプリケーションが OS の管理するリソースにアクセスするには、OS が提供する API (Application Program Interface)) を利用する。この API の利用方法は OS により確定しており、API を利用する実行コード部を判別することができる。本発明では、リソースへのアクセスに必要なすべての API を監視する監視ルーチンを設け、アプリケーションが API を利用する前に、その実行コード部を変更するか、API 処理の入りを監視ルーチンと置き換えることで、API 利用時に監視ルーチンが利用されるようにする。監視ルーチンは、アプリケーションが求める API を処理するか、もしくは API の処理をせずに不正命令としてアプリケーションに結果を返す。本発明のリソース管理プログラムによって拡張したアクセス権の管理は、OS の管理とは別に本プログラムが管理し、アクセス権の種類別に監視ルーチンを設ける。この方法により、リソースを不正に利用するアプリケーションから、そのアクセスを制限する。

【 0 0 1 2 】

図 2 は、本発明に係るリソース管理プログラム 2 0 3 の構成及び API 監視／制御の概念を示す図であり、リソース管理プログラム 2 0 3 は API 監視コントローラ (API 監視 CTRL) 2 0 3 1、APL 監視コントローラ (APL 監視

CTRL) 2 0 3 2、アクセス制御コントローラ (アクセス制御CTRL) 2 0 3 3、OS監視コントローラ (OS監視CTRL) 2 0 3 4 から構成されており、リソースアクセス要求を出すアプリケーション 2 0 2 1 や画面キャプチャなどのOS機能操作 2 0 2 2 を備える一般的なアプリケーションからなるユーザ環境 2 0 2 と汎用OS 2 0 1 との間に位置し、汎用OS 2 0 1 およびユーザ環境 2 0 2 が提供するリソースに対する要求を監視するようになっている。

なお、汎用OS 2 0 1 は、OSが管理するリソース 2 0 1 1 と、OSがアプリケーション 2 0 2 1 に提供しているAPI群 2 0 1 2 を備える。

【0 0 1 3】

本発明に係るリソース管理プログラム 2 0 3 におけるAPI監視CTRL 2 0 3 1 は、アクセス制御を行なうのに必要な全てのAPIを監視するモジュールである。また、APL監視CTRL 2 0 3 2 は、アプリケーション 2 0 2 1 ンが保持しているリソースを記憶するモジュールである。アクセス制御CTRL 2 0 3 3 はアクセスが許可されているかを判断するモジュールであり、アクセス権管理テーブル 2 0 3 5 を備える。また、OS監視CTRL 2 0 3 4 は、汎用OS 2 0 1 の機能によってリソースへアクセスする操作を監視するモジュールである。

【0 0 1 4】

アクセス権限テーブル 2 0 3 5 は、図 3 に示すように、リソース指定情報 2 0 3 5 1、条件 2 0 3 5 2、n 個のアクセス権情報 2 0 3 5 3 ~ 2 0 3 5 n をリソース毎に登録可能に構成されている。

リソース指定情報 2 0 3 5 1 は、汎用OS 2 0 1 が管理しているリソースのうち、特定のものを指定するための情報であり、例えば、ファイルの場合はファイル名やファイルIDなどの情報が登録される。通信データの場合は、ホスト名、ポート番号、IPアドレスなどが登録され、メモリの場合は、そのオブジェクトを示すオブジェクト名、アドレスなどが登録される。また、外部出力装置の場合は、そのデバイスドライバを示すデバイス名などが登録される。

条件 2 0 3 5 2 は、アクセス権が有効となる条件またはその組み合わせをしめすものであり、例えばユーザ名/ID、グループ名/ID、時刻、使用アプリケーションなどが登録される。

アクセス権情報 2 0 3 5 3 ~ 2 0 3 5 n は、既存環境で定義されていない拡張したアクセス権のうち、指定したリソースに付加した権限を示すものであり、例えば他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限（Windowsではクリップボードなど）、画面ハードコピー権限、使用アプリケーションの限定（特定アプリケーション以外での使用禁止やメール添付の禁止）などが登録される。

なお、一般的に、リソースへのアクセスは複数の A P I によって行われることがあり、その場合はリソース指定情報は O S が管理する I D（ハンドルなど）に変換されることがある。その場合、リソース管理プログラム 2 0 3 の内部においては、リソース指定情報とその I D は同一視するようにしている。

【 0 0 1 5 】

このような構成に係るリソース管理プログラム 2 0 3 の処理について、図 2 の ①～⑨で示す情報伝達手順に従って説明する。

①アプリケーション 2 0 2 1 からリソースへのアクセス要求があれば、アクセス制御 C T R L 2 0 3 3 に伝える。

②アクセス制御 C T R L 2 0 3 3 は、アクセス権限チェックを行なう際、必要に応じて、アプリケーション 2 0 2 1 が保持しているリソースの情報を A P L 監視 C T R L 2 0 3 2 から取得する。

③アクセスを拒否する条件として 2 通りあるが、第 1 の条件 A（アクセス拒否 A）では、上記①のアクセス要求に対してアクセス権限チェックを行なう。権限がない場合、アプリケーション 2 0 2 1 が発行した A P I の処理を行わずに、結果としてアクセス違反のエラーを返す。

④第 2 の条件 B（アクセス拒否 B）では、②のアクセス要求に対してアクセス権限チェックを行なう。権限がなく、かつ、アプリケーション 2 0 2 1 が発行した A P I の結果としてエラーを返すことができない場合、アプリケーション 2 0 2 1 が要求したリソースへの処理を行わずに、リソース管理プログラム 2 0 3 が予め用意したダミーのリソースへのアクセス要求に代えて、A P I の処理を行なう。

その結果、アプリケーション 2 0 2 1 は要求に成功したように動作するが、実

際には要求したリソースにアクセスできない。

【 0 0 1 6 】

⑤アクセス要求①に対してアクセス権限チェックを行った結果、権限がある場合、アプリケーション 2 0 2 1 が発行した A P I の処理をそのまま汎用 O S 2 0 1 に伝え、その結果をアプリケーション 2 0 2 1 に返す。

⑥上記⑤の処理によって、A P I が成功し、かつ、その A P I によってアプリケーション 2 0 2 1 がリソースを保持する場合は、A P L 監視 C T R L 2 0 3 2 に伝える。A P L 監視 C T R L 2 0 3 2 はアプリケーション 2 0 2 1 と保持しているリソースの対応を登録する。

アプリケーション 2 0 2 1 がリソースの解放要求 A P I を発行し、かつその A P I が成功した場合も、A P L 監視 C T R L 2 0 3 2 に伝える。A P L 監視 C T R L 2 0 3 2 はアプリケーション 2 0 2 1 と保持していたリソースの対応を抹消する。

⑦ O S 標準機能の操作によって、リソースへのアクセス要求があれば、アクセス制御 C T R L 2 0 3 3 に伝える。

⑧アクセス要求⑦に対してアクセス権限チェックを行なう。権限がない場合、⑦の操作を無視する。

⑨アクセス要求⑦に対してアクセス権限チェックを行なう。権限がある場合、⑦の操作を汎用 O S 2 0 1 に伝える。

【 0 0 1 7 】

図 4 は、目的とするリソースに対するアクセス権限がある場合に、そのリソースを解放するまでのアプリケーション 2 0 2 1、リソース管理プログラム 2 0 3、汎用 O S 2 0 1 のやり取りを示した A P I の監視及び制御の第 1 の基本型（1）のシーケンス図である。

この第 1 の基本型（1）では、アプリケーション 2 0 2 1 から目的のリソースへのアクセス要求があった場合（ステップ 4 0 1）、リソース管理プログラム 2 0 3 はアクセス権があるかチェックし（ステップ 4 0 2）、アクセス権がある場合（ステップ 4 0 3）、汎用 O S 2 0 1 にアプリケーション 2 0 2 1 が発行した A P I をそのまま伝える。汎用 O S 2 0 1 は、O S 本来の A P I 処理を行なう（

ステップ404)。

リソース管理プログラム203は、APIが成功した場合、アプリケーション2021がそのリソースを保持しているという情報を登録する(ステップ405)。そして、汎用OS201からのAPI結果をそのままアプリケーション2021に返す(ステップ406)。これにより、リソースへのアクセス完了となる(ステップ408)。

【0018】

この後、アプリケーション2021から保持しているリソースの解放要求が発行された場合(ステップ408)、リソース管理プログラム203はその解放要求を汎用OS201に伝える。汎用OS201は、OS本来のAPI処理を行なう(ステップ409)。リソース管理プログラム203は、APIが成功した場合、アプリケーション2021がそのリソースを保持しているという情報を解除する(ステップ410)。そして、汎用OS201からのAPI結果をそのままアプリケーション2021に返す(ステップ411)。これにより、保持しているリソースの解放完了となる(ステップ412)。

【0019】

図5は、目的とするリソースに対するアクセス権限がなかった場合に、そのアクセスが拒否されるまでのアプリケーション2021、リソース管理プログラム203、汎用OS201のやり取りを示したAPIの監視及び制御の第2の基本型(21)のシーケンス図である。

この第2の基本型(2)では、アプリケーション2021から目的のリソースへのアクセス要求があった場合(ステップ501)、リソース管理プログラム203はアクセス権があるかチェックし(ステップ502)、アクセス権がなかった場合(ステップ503)、アクセス違反エラーをアプリケーション2021に返す(ステップ504)。これにより、リソースへのアクセス完了となる(ステップ505)。

また、アプリケーション2021がアクセス違反エラーに対応していないものにあっては、アプリケーション2021から目的のリソースへのアクセス要求があった場合(ステップ506)、リソース管理プログラム203はアクセス権が

あるかチェックし（ステップ507）、アクセス権がなく、かつ、アプリケーション2021がアクセス違反エラーに対応していない場合（ステップ508）、リソース管理プログラム203が予め用意したダミーのリソースへのアクセス要求に置き換え、汎用OS201に渡す（ステップ509）。

【0020】

汎用OS201は、OS本来のAPI処理を行なう（ステップ510）。リソース管理プログラム203は、汎用OS201からのAPI結果をそのままアプリケーション2021返す（ステップ511）。この結果、目的のリソースへのアクセス完了となるが、ダミーリソースのため、実質的には何も行われない。

【0021】

本発明は、以上のようにしてアクセス権限のないリソースへのアクセスを制限するものであるが、汎用のOSであるWindowsとUNIXの場合のAPIを例に挙げて説明する。

まず、ファイルへの複製を禁止する例について説明する。

ファイルへの複製については、従来、読み込み許可ファイルはファイルのコピーが可能であり、その結果オリジナルが複数存在したり、別媒体にて持ち出すことが可能であった。本発明では、ファイルコピーを実現するAPIを監視／制御することにより、権限のないファイルのコピーを禁止する。その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。なお、以下で例示するAPIの機能については、各種の文献で公開されているので、その詳細な説明は省略する。

（1）ファイルオープン／作成API

CreateFileA

CreateFileW

OpenFile

#lopen

#lcreat

GetOpenFileNameA

GetOpenFileNameW

GetSaveFileNameA

GetSaveFileNameW

(2) ファイルクローズAPI

CloseHandle

#lclose

(3) ファイルコピー／移動API

CopyFileA

CopyFileW

MoveFileA

MoveFileW

MoveFileExA

MoveFileExW

DeleteFileA

DeleteFileW

DragQueryFileA

DragQueryFileW

UNIXの場合、監視／制御するAPIとしては次のものがある。

(1) ファイルオープン／作成API

open

creat

(2) ファイルクローズAPI

close

(3) ファイルコピー／移動API

rename

【0022】

このようなAPIの監視によってファイルへの複製を禁止する場合、具体的な方法として3つの方法がある。

＜方法1＞（ファイルオープン中に複製処理を行なうことが判明している場合）

アプリケーションが、複製権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションが別のファイルを作成することを拒否する。

＜方法2＞（ファイルクローズ後に複製処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、複製権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、複製権限のあるファイルをオープンするまで、そのアプリケーションが別のファイルを作成することを拒否する。

＜方法3＞（ファイルクローズ後に複製処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、複製権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションが別のファイルを作成することを拒否する。

なお、いずれの方法であっても、別に作成されるファイルによって複製が残ることがないと判明している場合（一時ファイルなどの作成）は拒否しない。

【 0 0 2 3 】

次に、特定ファイルまたは全ての印刷を禁止する例について説明する。

従来、印刷機能を実装したアプリケーションによって、ファイルの内容を印刷し、外部に持ち出すことは可能であった。本発明では、印刷を実現するAPIを監視／制御することにより、権限のないファイルの印刷を禁止する。またFAXなどその他の外部出力装置についても、それぞれのデバイスを監視／制御することにより、同様に禁止する。その場合に、Windows及びUNIXにおいて監視／制御するAPIとして次のものがある。

Windowsの場合

（1）デバイスオープンAPI

CreatedCA, CreatedCW

（2）デバイスクローズAPI

ReleaseDC, ClosePrinter

（3）プリンタ選択／APL処理API

OpenPrinterA

OpenPrinterW

GetPrinterA

GetPrinterW

SetPrinterA

SetPrinterW

SendMessageA

SendMessageW

PostMessageA

PostMessageW

UNIXの場合

(1) デバイスオープンAPI

open

(2) デバイス制御API

ioctl

(3) デバイスクローズAPI

close

【0024】

このようなAPIの監視によって印刷を禁止する場合、具体的な方法として3つの方法がある。

＜方法1＞（ファイルオープン中に印刷処理可能なことが判明している場合）

アプリケーションが、印刷権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープンを拒否する。

＜方法2＞（ファイルクローズ後に印刷処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、印刷権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、印刷権限のあるファイルをオープンするまで、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープン

を拒否する。

＜方法 3＞（ファイルクローズ後に印刷処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、印刷権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープンを拒否する。

【 0 0 2 5 】

次に、外部装置の利用を禁止する例について説明する。

従来、OSに装備されている機能や外部装置そのものに権限を付加することは、一般的にはできなかった。本発明では、監視／制御すべきAPIを限定できる機能の指定や、外部装置利用の指定することにより、その利用を禁止する。その場合に、Windows及びUNIXにおいて監視／制御するAPIとして次のものがある。

Windowsの場合

(1) デバイスオープンAPI

CreateFileA

CreateFileW

OpenFile

#lopen

#lcreat

(2) デバイスクローズAPI

CloseHandle

#lclose

UNIXの場合

(1) デバイスオープンAPI

open

(2) デバイス制御API

ioctl

(3) デバイスクローズAPI

close

【 0 0 2 6 】

このような A P I の監視によって印刷を禁止する場合、具体的な方法として次の方法がある。

＜方法＞

アクセス権限テーブルにて、特定の条件のもとに特定デバイスの使用を禁止されている場合、そのデバイスの利用を以下の方法で拒否する。そのデバイスのデバイス名をもってデバイスオープン A P I 要求があった場合、アクセス禁止エラー、もしくはデバイスが存在しないというエラーを返すことで要求を拒否する。

【 0 0 2 7 】

次に、ファイル内の一部のデータまたは全ての複写を禁止する例について説明する。

従来、アプリケーションによってファイルを画面表示した結果、その内容のすべてまたは一部を O S の機能によって複写またはオブジェクトをいう単位で別ファイルに埋め込むことが可能であった。

本発明では、転写や埋め込み機能を実現する A P I （クリップボードの A P I 、 O L E の A P I など）を監視／制御することで、権限のない流用を禁止する。その場合に、Windowsにおいて監視／制御する A P I として次のものがある。

Windowsの場合

（ 1 ）複写／埋め込み A P I

OpenClipboard
SetClipboardData
GetClipboardData
GetOpenClipboardWindow
OleCreate
OleCreateEx
OleCreateFromFile
OleCreateFromFileEx
OleCreateFromData

OleCreateFromDataEx
 OleCreateLink
 OleCreateLinkEx
 OleCreateLinkFromData
 OleCreateLinkFromDataEx
 OleCreateLinkToFile
 OleCreateLinkToFileEx
 CloseClipboard

【 0 0 2 8 】

このような A P I の監視によって複写を禁止する場合、具体的な方法として 4 つの方法がある。

＜方法 1＞（ファイルオープン中に複写処理可能なことが判明している場合）

アプリケーションが、複写権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

＜方法 2＞（ファイルクローズ後に複写処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、複写権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、複写権限のあるファイルをオープンするまで、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

＜方法 3＞（ファイルクローズ後に複写処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、複写権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

＜方法 4＞（複写権限のないファイルを埋め込みオブジェクトとして取り込む

場合)

複写権限のないファイルを取り込む処理を行なう際に、オブジェクトの登録もしくはそのオブジェクトの取得APIにおいて、アクセス違反のエラーを返すか、空データを登録あるいは取得することで、処理要求を拒否する。

【0029】

次に、ネットワークを介してファイルが外部へ流出することを禁止する例について説明する。

従来、ファイルコピー以外に、FTPプログラムのように、ネットワークを介してファイルを外部へ転送することは可能であった。本発明では、ネットワークリソースにアクセスするAPIを監視／制御することで、権限のないファイルを使用中のアプリケーションから外部への流出を禁止する。その場合に、Windows及びUNIXにおいて監視／制御するAPIとして次のものがある。

(1) Windowsの場合

WSAStartup
accept
bind
connect
gethostbyname
gethostbyaddr
getprotobyname
getprotobynumber
getservbyname
getservbyport
getpeername
getsockname
gethostname
getsockopt
setsockopt
recv

recvfrom

socket

select

send

sendto

WSASend

WSASendTo

WSAAsyncSelect

WSAAsyncGetHostByAddr

WSAAsyncGetHostByName

WSAAsyncGetProtoByNumber

WSAAsyncGetProtoByName

WSAAsyncGetServByPort

WSAAsyncGetServByName

WSACancelAsyncRequest

WSASetBlockingHook

WSAUnhookBlockingHook

WSACleanup

closesocket

shutdown

(2) UNIXの場合

accept

bind

connect

gethostbyname

gethostbyaddr

getprotobyname

getprotobynumber

getservbyname

getservbyport

getpeername

getsockname

gethostname

getsockopt

setsockopt

recv

recvfrom

socket

select

send

sendto

closesocket

shutdown

【 0 0 3 0 】

このようなAPIの監視によって外部への流出を禁止する場合、具体的な方法として3つの方法がある。

＜方法1＞（ファイルオープン中に出力処理可能なことが判明している場合）

アプリケーションが、外部出力権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションからの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

＜方法2＞（ファイルクローズ後に出力処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、出力権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、出力権限のあるファイルをオープンするまで、そのアプリケーションの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

＜方法3＞（ファイルクローズ後に出力処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、出力権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

ただし、その通信によってデータ出力されないことが判明している場合は、拒否しない。

【 0 0 3 1 】

次に、ファイルの内容のイメージを取得することを禁止する例について説明する。

OSの機能として画面全体や一部、またはウインドウ単位のハードコピーをイメージデータとして取得することが、一般的には可能であり、従来、そのイメージデータを流用、持ち出しすることができた。本発明では、画面内のイメージデータ取得APIを監視／制御することで、イメージデータ取得を禁止する。その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。

(1) デバイスオープンAPI

GetWindowDC

WindowFromDC

GetDC

GetDCEX

GetDesktopWindow

GetDeviceCaps

CreateDCA

CreateDCW

(2) イメージ取得API

BitBlt

StretchBlt

(3) デバイスクローズAPI

DeleteDC

ReleaseDC

【 0 0 3 2 】

このようなAPIの監視によってイメージを取得することを禁止する場合、具体的な方法として3つの方法がある。

＜方法1＞（画面全体のハードコピーを拒否する場合）

現在画面上に表示されているウィンドウを所有しているアプリケーションが、ハードコピー取得権限のないファイルを保持している場合、画面全体のハードコピー取得を拒否する。画面全体のハードコピーは、画面全体を管理しているウィンドウ（Windowsの場合はデスクトップウィンドウ）を監視することで、＜方法2＞と同じ。

WindowsにおけるDirectDrawなど、画面全体のハードコピーを取得するAPIが存在すれば、同様に拒否する。

さらに、ディスプレイデバイスからVRAMイメージを取得するアプリケーションに対しては、それを拒否する。

＜方法2＞（ウィンドウのハードコピーを拒否する場合）

現在画面上に表示されているウィンドウを所有しているアプリケーションが、ハードコピー取得権限のないファイルを保持している場合、そのウィンドウのハードコピー取得を拒否する。ウィンドウが画面上に表示されているかは、ウィンドウの状態を監視することで行なう。

また、ハードコピー取得の拒否は、そのウィンドウに関連付けられたデバイスコンテキストからのイメージコピーを拒否することで行なう。

＜方法3＞（画面の一部のハードコピーを拒否する場合）

ハードコピーを取得する領域が判断できる場合は、＜方法1＞における条件を、取得領域が対象となるウィンドウと重なる時とし、以降は＜方法1＞と同じ。また領域が判断できない時は、＜方法1＞と同じ。

【0033】

次に、ファイル種別毎に利用アプリケーションを限定する例について説明する。

従来、アプリケーション利用に制限がないため、参照以外の目的でファイルにアクセス可能であった。本発明では、ファイルごとに利用アプリケーションを限定できる。その場合に、Windowsにおいて監視／制御するAPIとして次のものが

ある。

(1) ファイルオープン A P I

CreateFileA

CreateFileW

OpenFile

#lopen

#lcreat

(2) ファイルクローズ A P I

CloseHandle

#lclose

(3) プロセス管理 A P I

WinExec

CreateProcessA

CreateProcessW

ExitProcess

U N I X の 場 合

(1) ファイルオープン A P I

open

(2) ファイルクローズ A P I

close

【 0 0 3 4 】

このような A P I の監視によって利用アプリケーションを限定する場合、具体的な方法として次の方法がある。

<方法>

アプリケーションがファイルをオープンする際、そのファイルの権限をチェックし、許可されたアプリケーションでない場合はアクセス違反エラーを返すことで、オープン要求を拒否する。

次に、O S の特定の機能の利用を禁止する例について説明する。

従来、O S に装備されている機能に権限を付加することは、一般的にはできな

かった。本発明では、監視／制御すべきAPIを限定する機能を指定することで、その利用を禁止することができる。例えば、ファイルのタイムスタンプやシステム日時の変更を禁止するなどである。その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。

(1) ファイルのタイムスタンプ変更API

SetFileTime

(2) システム日時の変更API

SetSystemTime

SetSystemTimeAdjustment

【0035】

このようなAPIの監視によってOSにおける特定の機能の利用を禁止する場合、具体的な方法として次の方法がある。

<方法>

特定の条件下で禁止されているAPIが発行された際に、アクセス違反エラーを返すか、実際の処理を行わずに（ダミー処理）正常リターンすることで、禁止されているAPI（OS機能）を拒否する。

【0036】

次に、プロセス内メモリの参照または変更を禁止する例について説明する。

従来、アプリケーションが明示的に拒否しない限り、プロセス内メモリの参照／変更を禁止することができなかった。本発明では、プロセス内メモリの参照／変更APIを監視／制御することで、他のアプリケーションからの参照／変更を禁止することができる。

その場合に、Windowsにおいて監視／制御するAPIとして次のものがある。

(1) プロセス管理API

OpenProcess

CreateProcess

CloseHandle

(2) メモリ操作API

ReadProcessMemory

WriteProcessMemory

ReadProcessMemoryVlm

WriteProcessMemoryVlm

【 0 0 3 7 】

このような A P I の監視によってプロセス内メモリの参照または変更を禁止する印刷を禁止する場合、具体的な方法として次の方法がある。

<方法>

アクセスが禁止されているアプリケーションのプロセス内メモリにおいて、メモリ操作 A P I が要求された際に、アクセス違反エラーを返す。

次に、ブラウザに表示した W e b ページの印刷や保存や外部装置への出力を禁止する例について説明する。

従来、閲覧や再生のみを許可した W e b ページでも、実際にはブラウザソフトによって印刷や保存が可能であった。W e b ページをロードするためのネットワークリソースにアクセスする A P I を監視し、ブラウザが行う印刷や保存のアプリケーションを監視／制御することにより、印刷や保存や外部装置への出力操作を禁止することができる。その場合に、監視／制御する A P I として次のようなものがある。

Windowsの場合

(1) 通信 A P I

WSAStartup

accept

bind

connect

gethostbyname

gethostbyaddr

getprotobyname

getprotobyname

getservbyname

getservbyport

getpeername
getsockname
gethostname
getsockopt
setsockopt
recv
recvfrom
socket
select
send
sendto
WSASend
WSASendTo
WSAAsyncSelect
WSAAsyncGetHostByAddr
WSAAsyncGetHostByName
WSAAsyncGetProtoByNumber
WSAAsyncGetProtoByName
WSAAsyncGetServByPort
WSAAsyncGetServByName
WSACancelAsyncRequest
WSASetBlockingHook
WSAUnhookBlockingHook
WSACleanup
closesocket
shutdown

(2) その他、前述のファイル、印刷、外部装置への操作を禁止する場合の A

P I

UNIXの場合

(1)

accept

bind

connect

gethostbyname

gethostbyaddr

getprotobyname

getprotobynumber

getservbyname

getservbyport

getpeername

getsockname

gethostname

getsockopt

setsockopt

recv

recvfrom

socket

select

send

sendto

closesocket

shutdown

(2) その他、前述のファイル、印刷、外部装置への操作を禁止する場合の A

P I

【 0 0 3 8 】

このような通信 A P I を監視し、印刷や保存や外部装置への出力を禁止する方法として、次の方法がある。

まず、W e b ページ内に記述された禁止指定を読み取る。具体的には、h t t

p プロトコルまたは同等のプロトコルのデータを監視し、その中の Web ページデータ部分に印刷や保存の禁止指定タグが含まれていれば、その Web ページは印刷や保存が禁止されていると判断する。または、権限の獲得を利用者に求め、獲得できなかった場合に印刷や保存が禁止されていると判断する。しかし、獲得できた場合には、印刷や保存が禁止されていないものと判断する。すなわち、アクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定する。

印刷や保存や外部装置への出力が禁止されているページを表示しているブラウザが、印刷や保存を行なおうとした場合、前述した印刷やファイルの保存や外部装置への出力を禁止する方法を用いて、それを禁止する。

ここで説明した Web ページの例は、そのしくみの類似性により、容易にデジタルテレビジョンや携帯電話機、携帯型情報端末等のコンテンツにおいても利用できるものである。

【 0 0 3 9 】

次に、リソース管理プログラムを応用した例を示しておく。

図 6 は、リソース管理プログラム 2 0 3 が管理しているリソースのアクセス状況を履歴管理プログラム 6 0 1 に転送し、履歴管理データベース (DB) 6 0 2 に格納しておき、必要に応じて、図 8 に示すようなアクセス監視履歴として画面表示する構成を示したものである。通報プログラム 6 0 3 は、不正なアクセスがあった場合にシステム管理者の端末に対し、図 6 (b) で示すような内容の不正アクセス通知画面を送信し、表示させるものである。

なお、一般ユーザが不正アクセスを行なった場合には、図 6 (a) で示すような画面表示が行われる。

【 0 0 4 0 】

なお、上記の説明においては、アクセス権管理テーブルを参照してアクセス権限の有無を判定するようにしているが、コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定するようにすることもできる。

また、上記の説明において用いたネットワークリソースとは、通信媒体、デバ

イス、アクセスポイント、デジタルテレビジョンのチャンネル、通信データまたはコンテンツなど、OSが管理しているリソースのうちネットワークに関するものである。

【 0 0 4 1 】

以上のように、本実施形態においては、基本的には、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉し、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定し、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返し、アクセス権限がなければ当該操作要求を拒否するようにしたため、OSやプロセス（OSの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限することができる。

また、リソース管理プログラムを既存の環境に組み込むだけで、上述したような各種の不正アクセスを制限することができ、既存のアクセス権の範囲を拡張することが可能になる。

【 0 0 4 2 】

さらに、要求元のアプリケーションがアクセス違反に対応する機能を有していない場合であっても、ダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡すようにしたため、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することができる。

【 0 0 4 3 】 なお、リソース管理プログラムは、CD-ROM等のディスク型ストレージ、半導体メモリ及び通信ネットワークなどの各種の媒体を通じてコンピュータにインストールまたはロードすることができる。また、プログラム製品単体として、コンピュータユーザに提供することができる。

また、実施形態で例示したAPIについては、その一例を示しただけであって、OSのバージョンアップなどによって追加された場合でも容易に対応できるこ

とは言うまでもない。

【 0 0 4 4 】

【発明の効果】

以上の説明から明らかなように、本発明は、基本的には、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉し、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定し、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返し、アクセス権限がなければ当該操作要求を拒否するようにしたため、OSやプロセス（OSの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限することができる。

また、リソース管理プログラムを既存の環境に組み込むだけで、上述したような各種の不正アクセスを制限することができ、既存のアクセス権の範囲を拡張することが可能になる。

また、リソース制御プログラムを既存の環境に組み込むだけで、各種の不正アクセスを制限することができ、従来のアクセス権の範囲を拡張することが可能になる。

さらに、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することができるなどの効果が得られる。

【図面の簡単な説明】

【図 1】

本発明の実施環境の一実施形態を示すハードウェア構成図である。

【図 2】

本発明に係るリソース管理プログラムの機能構成及びOSとアプリケーションとの関係を示す図である。

【図 3】

アクセス管理テーブルのデータ構成例を示す図である。

【図 4】

本発明における A P I の監視／制御の第 1 の基本型を示すシーケンス図である。

【図 5】

本発明における A P I の監視／制御の第 2 の基本型を示すシーケンス図である。

【図 6】

アクセス違反があった場合に表示される画面の例を示す図である。

【図 7】

アクセス履歴を記録し、不正アクセスを通知する機能を加えた実施形態を示す図である。

【図 8】

アクセス監視履歴の表示画面の例を示す図である。

図である。

【図 9】

アクセス制限対象となるリソースの例を示す図である。

【符号の説明】

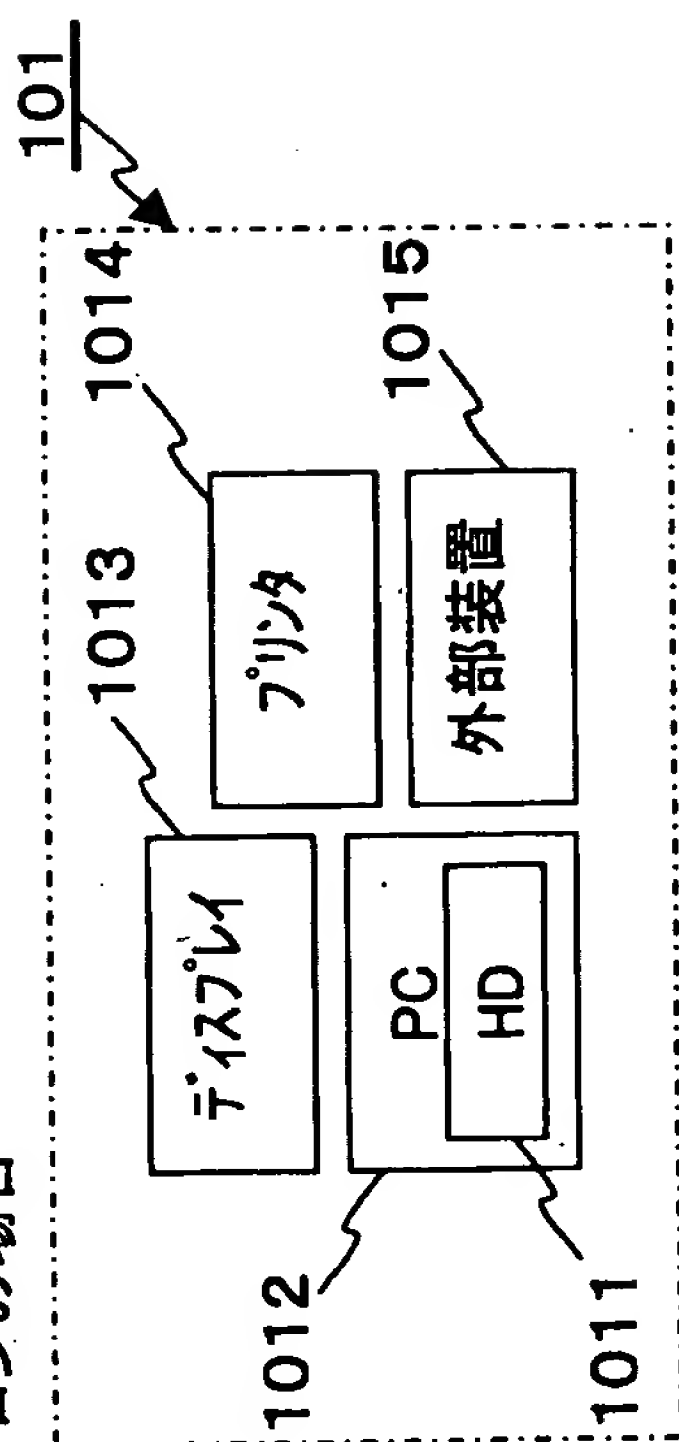
1 0 1 … コンピュータ、 1 0 2 … ネットワーク、 2 0 1 … 汎用 O S、 2 0 3 … リソース管理プログラム、 6 0 1 … 履歴管理プログラム、 6 0 3 … 通報プログラム、 2 0 3 1 … A P I 監視コントローラ、 2 0 3 2 … A P L 監視コントローラ、 2 0 3 3 … アクセス制御コントローラ、 2 0 3 4 … O S 監視コントローラ、 2 0 3 5 … アクセス権管理テーブル。

【書類名】

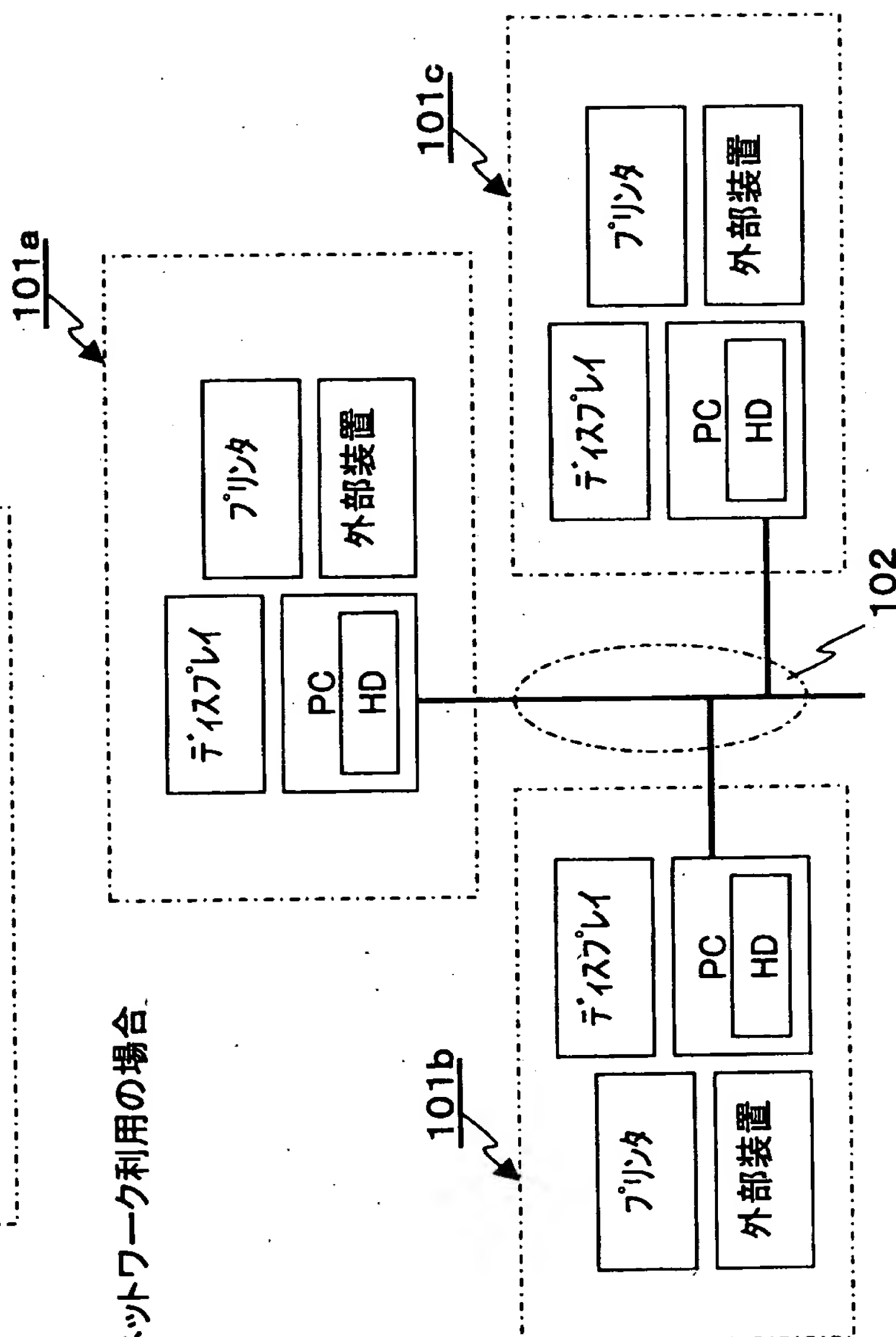
図面

【図 1】

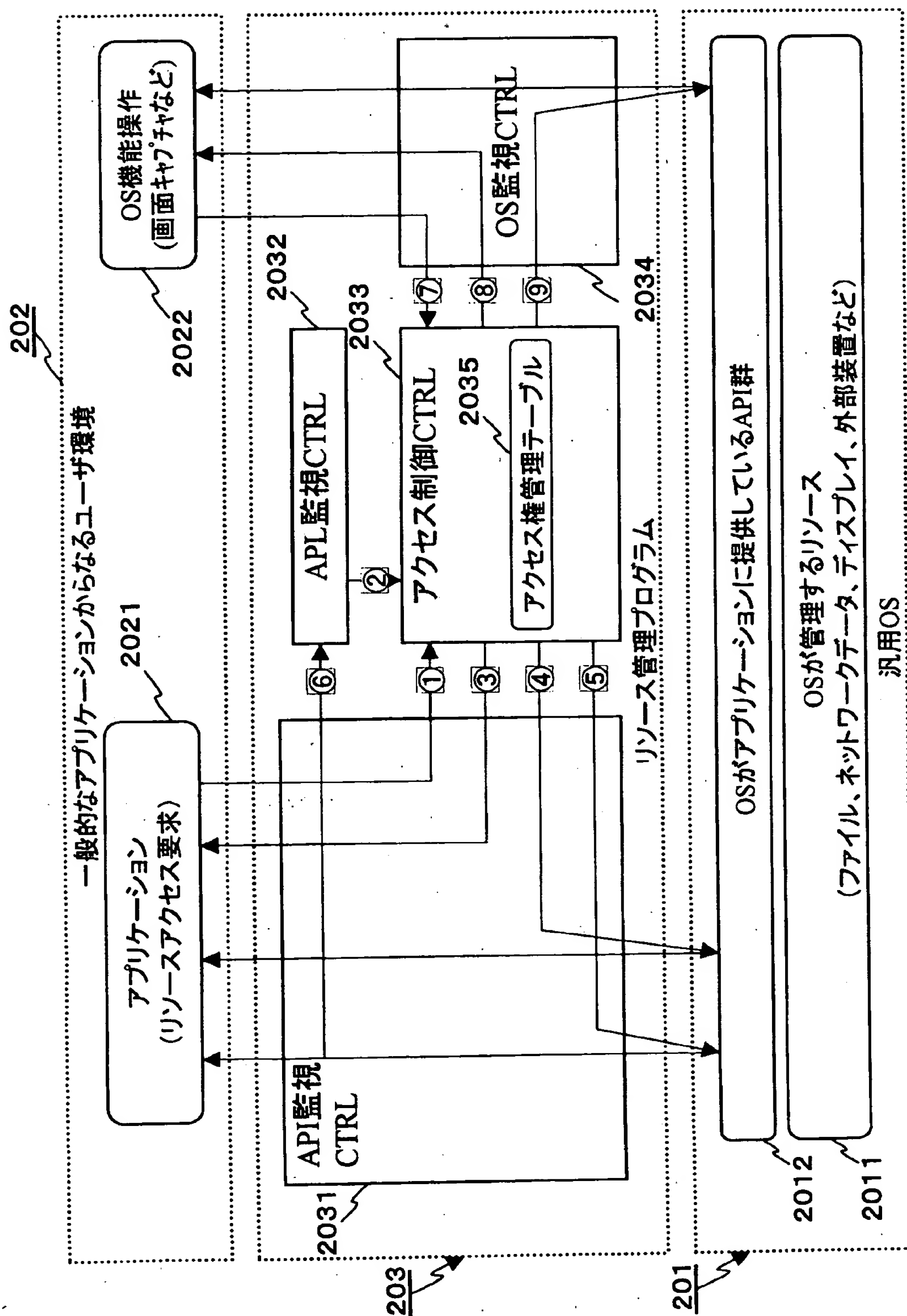
(a) スタンドアロンの場合



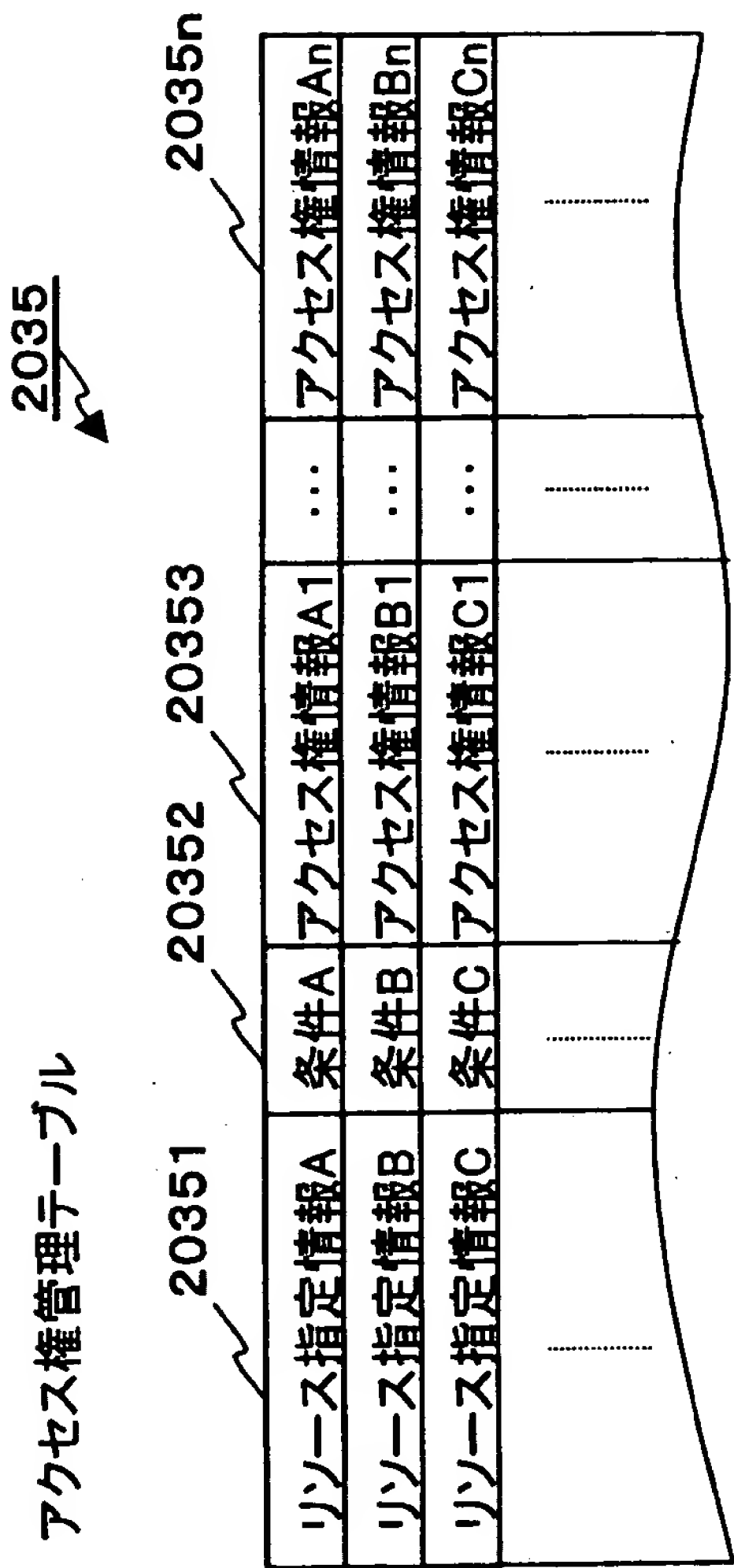
(b) ネットワーク利用の場合



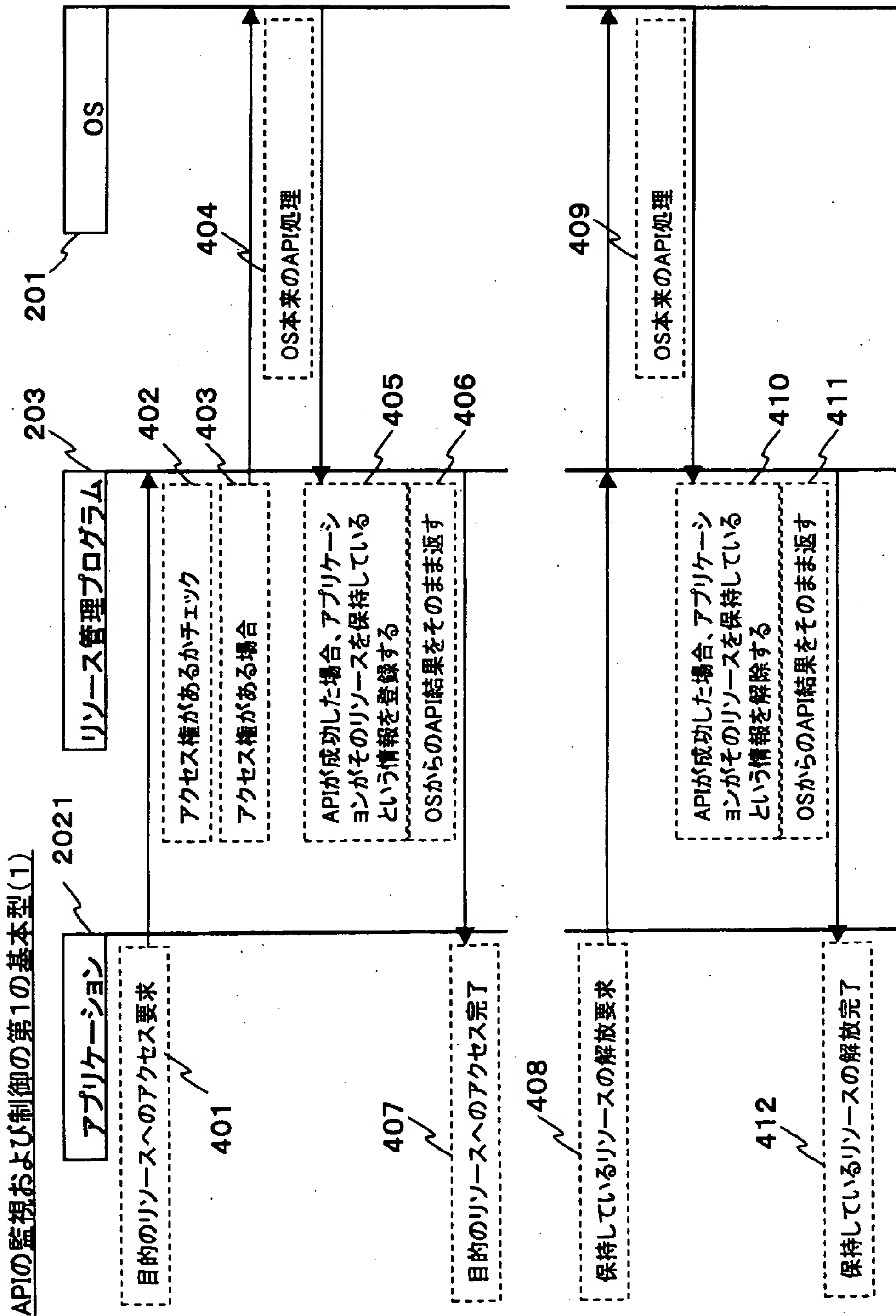
【圖 2】



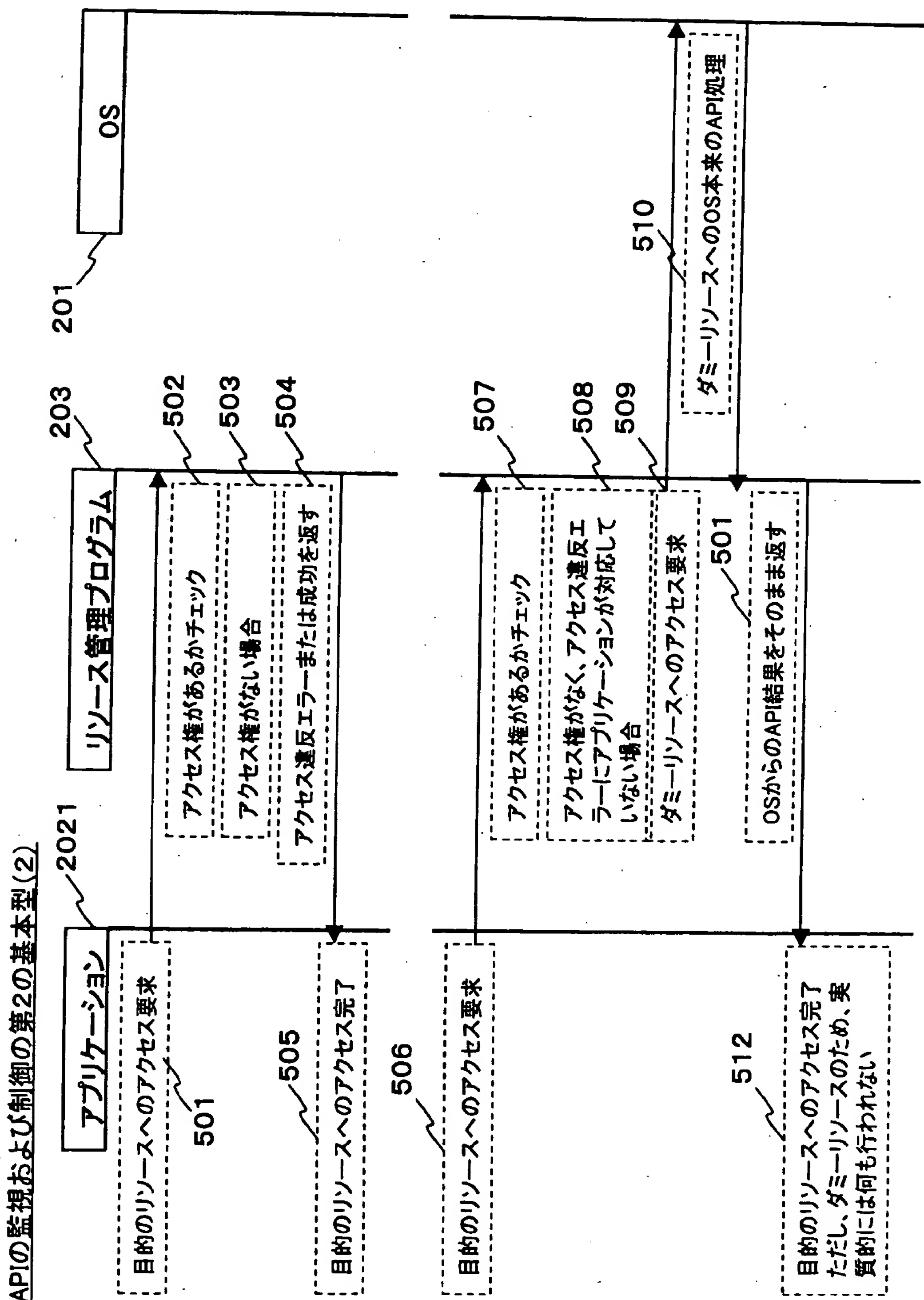
【図 3】



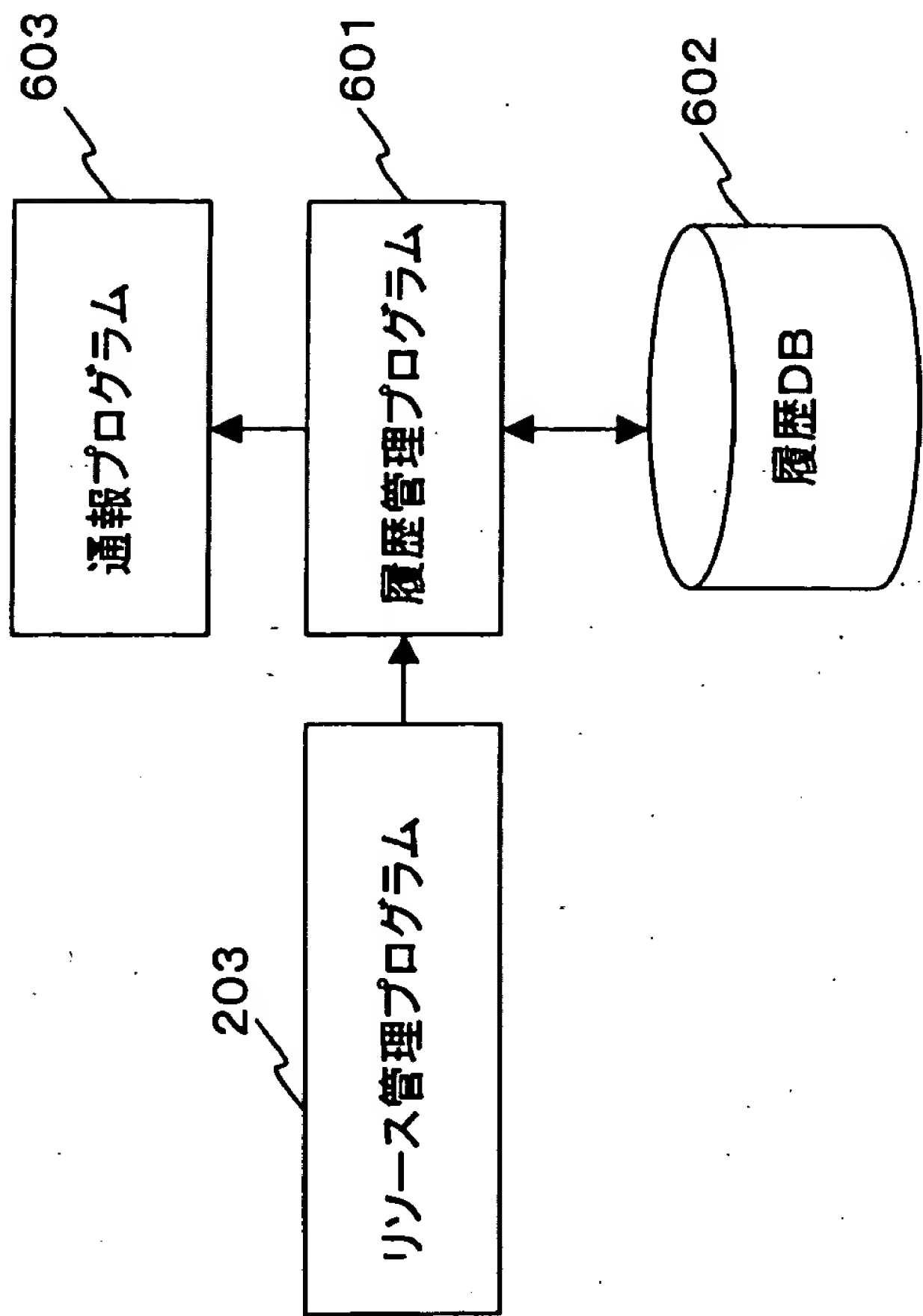
【図 4】



【図 5】

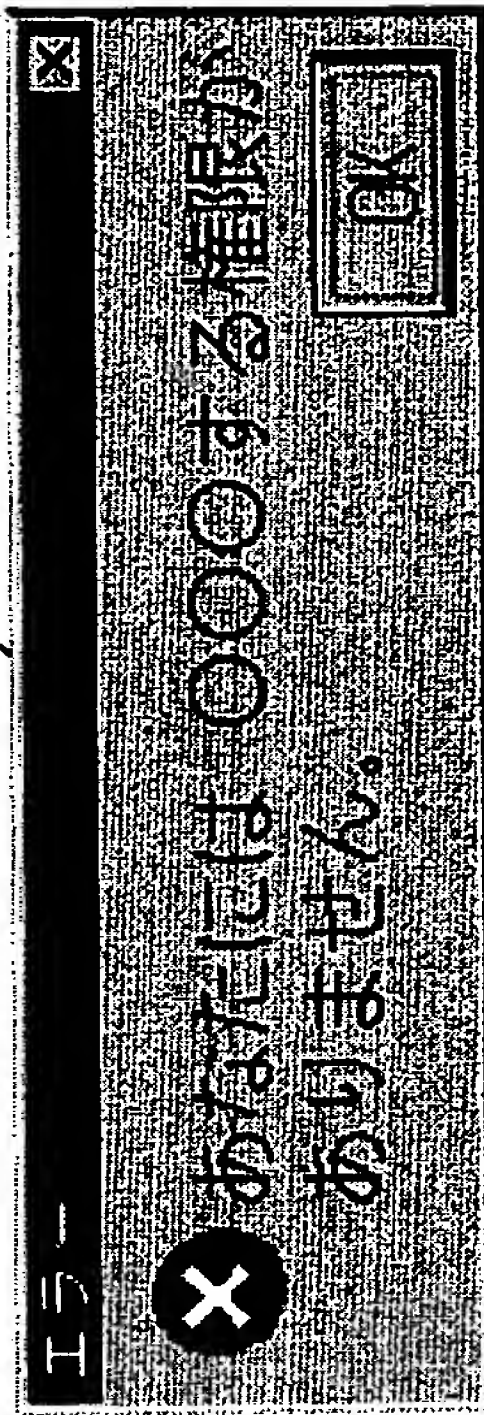


【図 6】



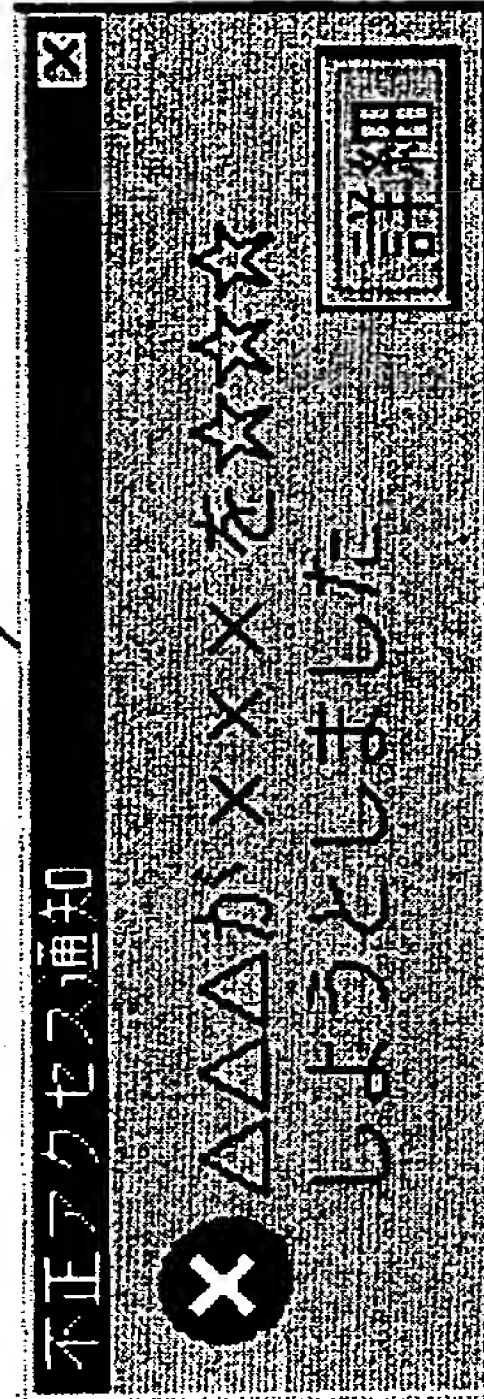
【図 7】

~ 701



(a)

~ 702



(b)

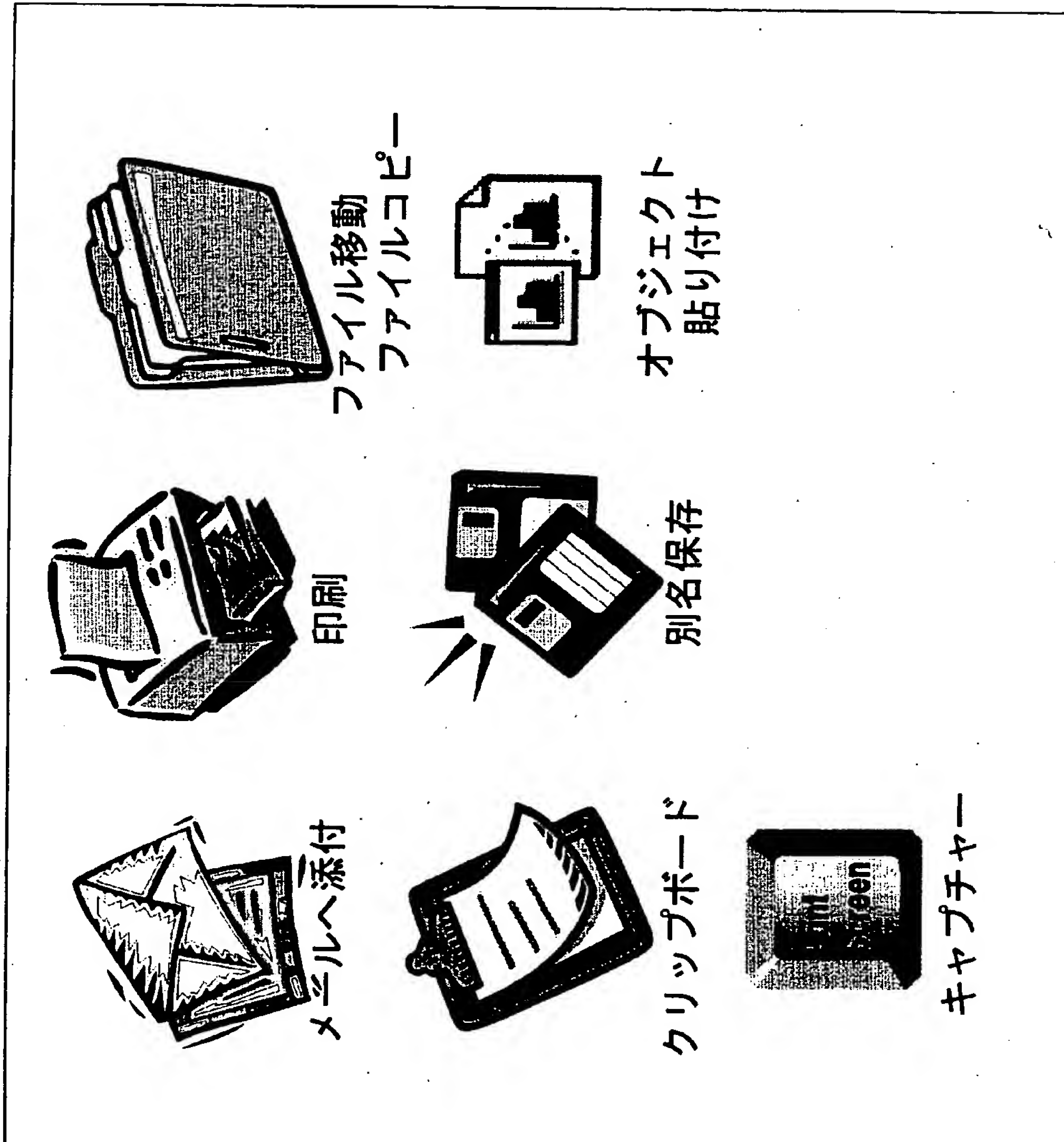
【図 8】

801

アクセス監視履歴					
ファイル(E) 編集(E) オプション(O) ヘルプ(H)					
全てのファイル 権限付きファイル					
ファイル名	利用者	操作	アクション	アクセス日時	場所
極秘文書	〇〇〇さん	ファイル更新	許可	00/01/01 0:00	総務...
顧客リスト	◆◆さん	印刷	拒否	00/01/01 0:00	営業...
開発ソース	☆☆さん	ファイルコピー	失敗	00/01/01 0:00	開発...
進行表	???さん	文書内部コピー	成功	00/01/01 0:00	企画...
査定表	●●さん	メール添付	拒否	00/01/01 0:00	人事...
財務報告書	□□□さん	画面キャプチャー	許可	00/01/01 0:00	経理...
会社案内	×××さん	ファイル移動	失敗	00/01/01 0:00	営業...
組織図				00	総務...

権限の無い◆◆◆さんが
顧客リストを印刷しようとしたので拒否しました。

【図 9】



【書類名】 要約書

【要約】

【課題】 OS やプロセスを変更することなく、アクセス権限のないユーザに対するリソースの操作を制限し、しかも既存環境における禁止または制限事項を拡張すること。

【解決手段】 ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉し、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定し、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返し、アクセス権限がなければ当該操作要求を拒否する。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 [500083226]

1. 変更年月日 2000年 2月25日
[変更理由] 新規登録
住 所 東京都中央区月島1丁目2番13号
氏 名 ハミングヘッズ株式会社